

Morgan Lewis

Andrew D. Lipman

Partner
+1.202.373.6003
andrew.lipman@morganlewis.com

December 10, 2021

VIA ECFS

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Dahua Ex Parte Meeting, Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program, ET Docket No. 21-232

Dear Ms. Dortch:



On December 9, 2021, Yanzi Li, Wayne Hurd, and Steven Mei of Dahua Technology USA Inc. ("Dahua"), as well as Andrew Lipman, Russell Blau, and JiaZhen (Ivon) Guo, counsels to Dahua, met with Brian Butler, George Tannahill, Howard Griboff, Jamie Coleman, Ira Keltz, Matthew Miller, Michael Ha, Muli Kifle, Paul Murray, Ronald Repasi, Ronald Williams, and Tom Struble of the Office of Engineering and Technology; Austin Randazzo, Debra Jordan, Erika Olsen, and Jeff Goldthorpe of the Public Safety Homeland Security Bureau; Justin Faulb of the Wireline Competition Bureau; and Douglas Klein of the Office of General Counsel via teleconference to discuss the above-captioned proceeding.

During the meeting, Dahua reiterated that Congress precisely defined the equipment and services that can be placed on the Covered List. These definitions do not encompass Internet of Things equipment, such as Dahua's video security cameras and systems, cables, displays, power supplies, alarm sensors, storage devices, intercoms, and access control solutions, among accessories (e.g., tripods, components, cables, SD cards) that operate outside of the broadband or telecommunications network.

Dahua also discussed the implications of the Secure Equipment Act of 2021 ("Secure Equipment Act") on this proceeding, stressing that the Secure Equipment Act only requires the Commission to adopt rules prohibit issuing equipment authorizations "for equipment that is on the list of covered communications equipment published by the Commission under section 2(a) of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1601(a))" and, therefore, the Commission's authority is limited within the scope of the Secure Networks Act. The Secure Equipment Act does not change the types of equipment and services on the Covered List. To the extent that the Covered List somehow reached Dahua's video camera equipment (which it

Morgan, Lewis & Bockius LLP

1111 Pennsylvania Avenue, NW
Washington, DC 20004
United States

 +1.202.739.3000
 +1.202.739.3001

cannot), the Commission is not authorized to prohibit equipment authorizations from being issued to Dahua equipment not used for public safety, security of government facilities, physical security surveillance of critical infrastructure, or other national security purposes.

Additionally, Dahua expressed that the Commission has no discretion to adopt any rule allowing revocation of already approved equipment just because it is on the Covered List. Revocation should only be considered for equipment that was not in compliance with the rules in effect at the time of its authorization.

Further, Dahua stressed that the Commission should not adopt its proposal to preclude Dahua from using the Supplier's Declaration of Conformity ("SDoC") process for non-covered equipment. The Secure Equipment Act does not address the Commission's authority with respect to anything that is not "covered" equipment, and pre-existing statutes do not authorize this regulation for the reasons stated in Dahua's comments and reply comments. Even if the Commission had such authority, the proposal would be arbitrary and capricious. Requiring Dahua to obtain third-party certification for all non-covered equipment would be overbroad, punitive, and not cost-effective. Dahua expressed its concerns on the enormous burden that such a requirement would impose on manufacturers, distributors, consumers, and small business owners in the U.S.

Finally, Dahua is willing to work with the Commission to address its concerns by, among other things, adhering to the Commission rules and ensuring conformity with the Commission technical standards, as well as providing documents associated with the SDoC and certification processes. As requested by the Commission during the meeting, Dahua states that its website containing certain product-specific SDoC information is available at https://dahuawiki.com/FCC_Documents.

Pursuant to Section 1.1206 of the Commission's rules, this letter is being filed in ECFS. A copy of the meeting presentation slides is attached hereto as Exhibit A. Please do not hesitate to contact the undersigned with any questions.

Respectfully submitted,

/s/ Andrew D. Lipman

Andrew D. Lipman
Morgan, Lewis & Bockius LLP
1111 Pennsylvania Avenue, N.W.
Washington, DC 20004
(202) 373-6033
andrew.lipman@morganlewis.com

Counsel to Dahua Technology USA Inc.

Marlene H. Dortch
December 10, 2021
Page 3

Exhibit A



Dahua Ex Parte Presentation

December 9, 2021 Meeting with the FCC

Dahua Technology USA Inc.

Yanzi Li
Wayne Hurd
Steven Mei

Morgan, Lewis & Bockius LLP

Andrew D. Lipman
Russell M. Blau
JiaZhen (Ivon) Guo

About Zhejiang Dahua Technology Co., Ltd. ("Dahua Technology")



Dahua Technology is a privately-owned company, founded in 2001

Certain state-owned enterprises hold minority stock interests, but are not represented on the Board of Directors or in company management

Dahua Technology is not controlled or operated by any government



Dahua Technology is publicly traded on the Shenzhen Stock Exchange

Dahua Technology does not produce telecommunications equipment

Dahua Technology produces peripheral equipment that are not different from other IoT devices such as video security cameras and systems, cables, displays, power supplies, alarm sensors, storage devices, intercoms, and access control solutions, among accessories (e.g., tripods, components, cables, SD cards).

About Dahua Technology USA Inc. (“Dahua”)



Dahua is a wholly owned subsidiary of Zhejiang Dahua Technology Co., Ltd. (“Dahua Technology”).

Dahua is founded in 2014 and headquartered in Irvine, California.

Dahua has had no past or pending government enforcement actions from the U.S. government

In the United States, Dahua directly employs 85 persons and distributes its products through a network of independent distributors, resellers, and retailers.

Dahua cooperates with more than 34 OEM partners and 8,000 registered dealers in the United States.

In the U.S., Dahua mainly markets video cameras (including IP, CVI, and Wi-Fi cameras), video recorders (including IP and CVI recorders); pan-tilt-zoom cameras; access control systems; intercom systems; monitors; and accessories (including power units and tripods).

Dahua users are not telecommunications carriers. Rather, they are consumers and small and medium-sized businesses such as jewelry stores, department stores, and pharmacies.

About Dahua Equipment

Dahua Equipment is all peripheral devices. Indeed, some Dahua Equipment (e.g., access control systems; intercom systems; monitors; and accessories) is not even video or telecommunications equipment.

Dahua Equipment can operate outside of the broadband or telecommunications network.

Dahua Equipment is not essential to broadband services and is not used for the provision of broadband or advanced communications services.

- End-users can deploy Dahua Equipment on a physically isolated network (*i.e.*, a private room with data stored in a local storage) not connected to the public network.
- End-users can deploy Dahua Equipment on a logically isolated network (*i.e.*, a local area network) with no access to the public network.
- Deploying Dahua Equipment on broadband or telecommunications networks will only congest other broadband or telecommunications traffic, increase network latency, and deteriorate the quality of service, so most users prefer a separate dedicated network.

About Dahua Equipment (cont'd)

Dahua follows stringent policies and procedures to protect against and remedy vulnerabilities in Dahua Equipment.

Dahua Equipment can be safeguarded by end-users through generally accepted cybersecurity best practices, similar to other IoT devices.

- Dahua does not collect information on its customers, except for limited user registration data.
- Dahua Equipment supports and end-users employ virtual private networks, firewall, access control, and end-to-end encryption to protect, monitor, and manage Dahua Equipment.
- Dahua Equipment requires end-users to set strong passwords that meet minimum criteria. Unlike many other IoT devices, Dahua Equipment must have a password customized by the end-user before being used.

The Covered List



Dahua respectfully disagrees with Congress' decision to identify its products as "covered equipment" in Section 889 of the National Defense Authorization Act for Fiscal Year 2019 (2019 NDAA).

But Dahua recognizes that the FCC was bound by that determination under Section 2(c)(3) of the Secure and Trusted Communications Network Act (STCNA).

Scope of the Covered List

Under Section 2 of STCNA, the Commission publishes a “list of covered communications equipment or services”.

SEC. 2. DETERMINATION OF COMMUNICATIONS EQUIPMENT OR SERVICES POSING NATIONAL SECURITY RISKS.

(a) PUBLICATION OF COVERED COMMUNICATIONS EQUIPMENT OR SERVICES LIST.—Not later than 1 year after the date of the enactment of this Act, the Commission shall publish on its website a list of covered communications equipment or services.

The Covered List lists: (1) *covered communications equipment and services*, not peripheral equipment and (2) *equipment and services*, not entities.

Purpose of the Covered List

Under Section 3 of STCNA, the Covered List is established to prohibit equipment on the Covered List from being procured or maintained with universal service support

SEC. 3. PROHIBITION ON USE OF CERTAIN FEDERAL SUBSIDIES.

(a) IN GENERAL.—

(1) **PROHIBITION.**—A Federal subsidy that is made available through a program administered by the Commission and that provides funds to be used for the capital expenditures necessary for the provision of advanced communications service may not be used to—

(A) purchase, rent, lease, or otherwise obtain any covered communications equipment or service; or

(B) maintain any covered communications equipment or service previously purchased, rented, leased, or otherwise obtained.

Dahua products are not generally used in the provision of services supported by federal universal service support.

Relevant Key Definitions

Legislative definitions are critical here as Congress was very precise in defining the equipment being covered, and the FCC's authority

Section 2(a)(2) of the Secure Equipment Act

Requires the Commission to “no longer review or approve any application for equipment authorization for equipment that is on the list of covered communications equipment or services.”

Section 7(5) of STCNA

The term “covered communications equipment or service” means any communications equipment or service that is on the list published by the Commission under section 2(a) of this Act.

Section 7(4) of STCNA

The term “communications equipment or service” means any equipment or service that is essential to the provision of advanced communications service.

Section 7(1) of STCNA

The term “advanced communications service” has the meaning given the term “advanced telecommunications capability” in section 706 of the Telecommunications Act of 1996 (47 USC 1302)

Section 706(d)(1)

The term “advanced telecommunications capability” is defined, without regard to any transmission media or technology, as high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology.

“Communications Equipment or Services”



Under STCNA, only “communications equipment or services” may be placed on the Covered List.

- Only equipment or services “essential to the provision of advanced communications service.”
- Therefore, only network equipment used by broadband service providers can be covered.

This does not include video cameras, video security systems, or accessories that are not even used in broadband networks or telecommunications services.

If Dahua were to produce any telecommunications network equipment (Dahua does not), that would be “covered” under the Section 889 determination and the STCNA Covered List; but no actual Dahua Equipment is covered.

Secure Equipment Act (SEA)

Section 2(a)(2) of the SEA requires the FCC to adopt rules providing “that the Commission will no longer review or approve any application for equipment authorization for equipment that is on the list of covered communications equipment or services published by the Commission under section 2(a) of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1601(a)).”

Only “communications equipment or services” on the Covered List is directly covered by the SEA.

The Commission does not have any discretion to change the criteria for listing covered communications equipment under the STCNA.

SEA's Impact on FCC Proposed Rules

In light of the SEA, the FCC has no discretion with respect to prohibiting **prospectively** authorization of equipment on the Covered List.

Likewise, it has no discretion to adopt any rule allowing revocation of already approved equipment because it is on the Covered List.

Revocation should only be considered for equipment that was not in compliance with rules in effect at the time of its authorization.

However, the SEA is silent as to the Commission's proposal to preclude entities who have equipment on the Covered List from using the Supplier's Declaration of Conformity (SDoC) process for non-covered equipment.

The FCC Should Not Prevent Dahua from Using SDoC



Dahua does not produce telecommunications network equipment, and so is very unlikely to seek authorization for any “covered communications equipment.”

If Dahua or a similarly-situated company did seek to circumvent the rules by using SDoC for covered equipment, the FCC could revoke that authorization.

Requiring Dahua to obtain third-party certification for *all* Dahua Equipment would be overbroad, punitive, and not cost-effective.

The FCC Should Not Prevent Dahua from using SDoC (cont'd)



The vast majority (~94%) of Dahua Equipment qualifies for the SDoC process.

Benefits would be minimal of excluding Dahua Equipment from the SDoC process, since little (if any) Dahua Equipment is covered communications equipment.

Costs to Dahua would be enormous (\$millions/year), and would have to be passed through to U.S. distributors and U.S. consumers.

The proposed rules can only be viewed as a punitive measure, specifically targeting Dahua and Dahua Equipment.

The FCC Cannot Justify the Enormous Burden

The FCC must conduct a cost-benefit analysis to justify the burden imposed on the manufacturers, consumers, and the FCC itself.

The additional costs on the manufacturers would have to be passed through to U.S. distributors and U.S. consumers.

FCC would need to significantly increase staff to process much greater volume of equipment certification applications.

Without sufficient resources, the proposed rules would subject *all* U.S. manufacturers to a much lengthier certification queue and slower the equipment authorization process across the board; these delays would hamper U.S. global competitiveness and economic growth.

The FCC Should Not Consider Revoking Existing Valid Authorizations



Revoking existing equipment authorizations would be hugely costly to the economy, and the real-world impact affects different sectors of the economy and affect hundreds of thousands, if not millions, of end users.

Small business owners will not be able to replace existing equipment with alternative affordable equipment manufactured by U.S. and EU manufacturers; U.S.- and EU- manufactured equipment is more expensive.

The Secure and Trusted Networks Reimbursement Program involves less than a hundred telecommunications carriers yet costs have ballooned to (at least) \$2 billion; whereas tens of thousands of dealers, distributors, resellers, and installers, and possibly millions of end-users will be affected by a “rip-and-replace” of video security equipment. Some small businesses will be forced to go out of business.

The proposed revocation would create significant confusion among dealers, distributors, resellers, installers, and end-users.

Dahua Is Willing to Work With the FCC to Address Its Concerns



Dahua has an office within the U.S. and is the responsible party for purpose of the SDoC process.

Dahua will adhere to the Commission rules and ensure conformity with the Commission's technical standards.

Dahua keeps copies of the documents prepared in relation to the SDoC and certification processes in the U.S.

Dahua is willing to provide documents associated with the SDoC process upon FCC's request.

Thank You